UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/520,274	01/18/2005	Eli Yanovsky	29238	9022

67801 7590 06/08/2010

MARTIN D. MOYNIHAN d/b/a PRTSI, INC.
P.O. BOX 16446
ARLINGTON, VA 22215

EXAMINER	
KANAAN, SIMON P	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
06/08/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/520,274	YANOVSKY, ELI	
	Examiner	Art Unit	
	SIMON KANAAN	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *5/21/2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is responsive to communication filed 01/04/2010 for application No: 10/520274.

2. Applicant's arguments have been considered but are moot based on the new grounds of rejection as shown below.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 19, 21, and 37 are rejected under 35 U.S.C. 102(b) as being anticipated by Atalla (US 5,960,086) hereinafter referred to as Atalla.

With respect to claim 37, Atalla discloses method of key management with at least one remote party, –Atalla, abstract and column 4, lines 20-25 lines, teaches creating identical keys at two different remote parties

comprising the steps of: sharing with said remote party a primary data stream, -Atalla, figure 7, item 71, teaches communication between two parties over an insecure network

using said primary data stream and identical settings at each party to form an identical randomizer at each party, -Atalla, figure 7, items 70 and 72, teaches using the data stream communication between two parties and randomizers at two different parties to create identical random session signatures at two different parties.

selecting parts of said primary data stream using said identical randomizer at each party to form identical derived data sources independently at each party, and -Atalla, figure 7, items 9 and 11, teaches creating identical data source of a session signature using the parts of the data stream and the identical random session signatures

using said derived data source to form identical cryptography keys separately at different parties at predetermined intervals. -Atalla, figure 7, items 9 and 11, teaches creating identical keys at two different parties independently and column 13, lines 42-50, teaches changing signatures which would generate new keys periodically so in predetermined intervals.

As per claim 1, Atalla discloses apparatus for use by a first party for key management for secure communication with a second party, said key management being to provide at each party, simultaneously remotely, identical keys for said secure communication without transferring said keys or components thereof over any communication link, –Atalla, abstract and column 4, lines 20-25 lines, teaches creating identical keys at two different remote parties without transferring keys or components thereof

the apparatus comprising: a datastream extractor, for obtaining from data exchanged between said parties a bitstream, -Atalla, figure 7, items 9 and 11, teaches creating identical data

source of a session signature using the parts of the data stream and the identical random session signatures

a random selector said selection setting defining a selection, from said bitstream, of a series of bits in accordance with a randomization within said random selector, said randomization seeded by said data exchanged between said parties, -Atalla, figure 7, items 9 and 11, teaches creating identical data source of a session signature using the parts of the data stream and the identical random session signatures

a key generator for generating a key for encryption/decryption based on said series of bits, thereby to manage key generation in a manner repeatable at said parties, without transferring said keys or components thereof over the communication link. -Atalla, figure 7, items 9 and 11, teaches creating identical keys at two different parties independently and column 13, lines 42-50, teaches changing signatures which would generate new keys periodically thereby keys are managed by the change in signatures which triggers a change in key.

With respect to claim 2, Atalla discloses apparatus according to claim 1, the random selector being operable to use results of said randomization as addresses to point to bits in said datastream – Atalla, column 3, lines 23-29, teaches selecting bytes and identifies addresses of each byte.

With respect to claim 19, Atalla teaches that said system being operable to provide key management for a symmetric cryptography algorithm. –Figure 7, teaches symmetric cryptography algorithm to generate keys

As per claim 21, Atalla discloses A system for providing key management between at least two separate parties, –Atalla, abstract and column 4, lines 20-25 lines, teaches creating identical keys at two different remote parties without transferring keys or components thereof

the system comprising a primary bitstream for exchange between said parties, and at each party: -Atalla, figure 7, items 9 and 11, teaches creating identical data source of a session signature using the parts of the data stream and the identical random session signatures

a selector for randomly selecting, at predetermined selection intervals, parts of said primary bitstream to form a derived bit source, each selector being operable to use said derived bit source, in an identical manner, to randomize said selecting, -Atalla, figure 7, items 9 and 11, teaches creating identical data source of a session signature using the parts of the data stream and the identical random session signatures

and a key generator for generating cryptography keys at predetermined key generating intervals using said derived bit source of a corresponding selection interval. -Atalla, figure 7, items 9 and 11, teaches creating identical keys at two different parties independently and column 13, lines 42-50, teaches changing signatures which would generate new keys periodically thereby keys are managed by the change in signatures which triggers a change in key.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3-4, 19-20, 22-23 and 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla in view of Seheidt et al. (US 5,375,169) hereinafter referred to as Seheidt.

With respect to claim 3, Atalla discloses apparatus according to claim 1,

But does not disclose said key generator operable to generate a new key after a predetermined number of message bits have been exchanged between said parties

However, Seheidt discloses said key generator operable to generate a new key after a predetermined number of message bits have been exchanged between said parties – Seheidt, column 8, lines 31-33, teaches new keys are generated every time a new message is communicated between parties

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Atalla with updating of keys of Seheidt to prevent compromise of the key.

With respect to claim 4, Atalla in view of Seheidt discloses apparatus according to claim 3, said predetermined number of message bits being substantially equal to a length in bits of said key – Seheidt, column 8, lines 33-34, teaches alternatively, the key may remain the same as long as the same parties are in communication.

With respect to claim 20, Seheidt teaches that being constructed modularwise such that said cryptography algorithm is exchangeable (In addition to the protection of the keys themselves, selecting the proper key sequence and increasing the frequency with which the key sequence is changed can enhance the security of this type of protection, col. 2, lines 2-6).

With respect to claim 22, Atalla in view of Seheidt teaches that said primary bitstream is obtainable as a stream of bits from a data communication process between said two parties (The key component is a pseudorandom sequence of bits with an appended error detection field which is mathematically calculated based on the pseudorandom sequence, abstract).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Atalla with updating of keys of Seheidt to prevent compromise of the key.

With respect to claim 23, Atalla in view of Seheidt teaches that teaches that said bits in said primary bitstream are separately identifiable by an address, and wherein said selector is operable to select said bits by random selection of addresses (The pseudorandom sequence is generated using known pseudorandom sequence generating means within the cryptographic engine 24, for example, through the use of serial shift registers having selected outputs modulo-2 added and fed forward, col. 6, lines 29-34)

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Atalla with updating of keys of Seheidt to prevent compromise of the key.

With respect to claim 38, Atalla in view of Seheidt teaches that said primary data source is obtainable as a stream of bits from a communication process between said two parties (The key component is a pseudorandom sequence of bits with an appended error detection field which is mathematically calculated based on the pseudorandom sequence, Abstract).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Atalla with updating of keys of Seheidt to prevent compromise of the key.

With respect to claim 39, Atalla view of Seheidt. teaches that said primary data source comprises a stream of data bits divisible into data units and comprising selecting at random from the data bits of each data unit (The pseudorandom sequence is generated using known pseudorandom sequence generating means within the cryptographic engine 24, for example, through the use of serial shift registers having selected outputs modulo-2 added and fed forward col.6, lines 29-35).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Atalla with updating of keys of Seheidt to prevent compromise of the key.

With respect to claim 40, Atalla view of Seheidt teaches that said bits in said data units are separately identifiable by addresses, and comprising selecting said bits by using said randomizer as an address pointer - Atalla, column 3, lines 23-29, teaches selecting bytes and identifies addresses of each byte.

With respect to claim 41, Atalla teaches that selecting is carried out by using identically set pseudorandom data generation at each party, and using said derived data source as a seed for said pseudorandom data generation, -Atalla, figure 7, items 9 and 11, teaches creating identical data source of a session signature using the parts of the data stream and the identical random session signatures, and teaches transmitting addresses so that the key generation can be seeded appropriately using addresses from the random number generator at each side.

With respect to claim 48, Seheidt teaches that in use to provide key management for a symmetric cryptography algorithm (An alternative to the public key system is a private key system known as a symmetric key system which is a cryptographic system using the same key for both encryption and decryption. This key is transmitted from the sender to the receiver over a secure channel in parallel with the encrypted message, col. 3, lines 38-44).

6. Claims 5-18, 24-30, 34 and 42-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla in view of Khamharn et al. (5,375,169) hereinafter referred to as Khamharn .

With respect to claim 5, Atalla doesn't teach that a control message for sending control messages to said remote party, thereby to indicate to said remote party a state of said apparatus to enable said remote party to determine whether said remote party is synchronized therewith to generate an identical key.

However, Khamharn teaches that transmitting at least a first message from the transmitter to the receiver; and, in response to the receiver receiving the first message, the receiver detecting the absence of synchronization between the transmitter and the receiver and performing a resynchronization procedure to restore synchronization between the transmitter and the receiver, see abstract.

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the above references with to perform and restore synchronization between the transmitter and the receiver.

With respect to claim 6, Khamharn teaches that a synchronized state determiner, for determining from control messages received from a remote party whether said apparatus is synchronized therewith to generate an identical key (The value stored in NSQN 66 is compared to SQN2 42 to determine what level of resynchronization may be required. Subsequent to a successful message 20 authentication, memory location SQN2 42 is updated to contain the value of SQN1 28 stored in NSQN 66, col. 5, lines 27-33).

With respect to claim 7, Khamharn teaches that a resynchronizer, associated with said synchronous state determiner, said resynchronizer having a resynchronization random selector

for selecting, from a part of said bitstream previously used by said random selector, a series of bits in accordance with a randomization seeded by said data exchanged between said parties (the random initial state is used as starting point, col. 3, lines 33-34), in the event of determination of synchronization loss, thereby to regain synchronization (Once synchronization is lost, the system does not respond and appears inoperative. Resynchronization is required to restore the system operation to normal, col. 1, lines 19-22).

With respect to claim 8, Khamharn teaches that said series of bits is a series of bits previously used by said random selector (the random initial state is used as starting point, col. 3, lines 33-34).

With respect to claim 9, Khamharn teaches that said control messager is operatively connected to said synchronous state determiner, thereby to include within said control messages a determination of synchronization loss (transmitting at least a first message from the transmitter to the receiver; and, in response to the receiver receiving the first message, the receiver detecting the absence of synchronization between the transmitter and the receiver and performing a resynchronization procedure to restore synchronization between the transmitter and the receiver, abstract).

With respect to claim 10, Khamharn teaches that said control messager is operatively connected with said resynchronizer, to control said resynchronizer to carry out said selection in the event of receipt of a message from said remote party that said remote party has lost

synchronization (A first resynchronization process occurs within synchronization window 44, a resynchronization area whereby, subsequent to a first message 20 reception, SQN1 28 received is greater than SQN2 42 by not more than K increments, col. 4, lines 17-21).

With respect to claim 11, Khamharn teaches that said data communication being arranged in cycles, said part of said bitstream being exchangeable in each cycle (Current systems require a manual sequence of operations for restoring synchronization, such as depressing lock and unlock buttons for a predetermined period of time and waiting for a lock cycle feedback, col. 1, lines 22-26).

With respect to claim 12, Khamharn teaches that said cycle being arranged into sub-units, each said cycle having an exchange point at its beginning for carrying out said exchange (CRC 32 which is a cyclic redundancy check code to permit receiver 18 t validate the integrity of message transmission, col. 3, lines 48-49).

With respect to claim 13, Khamharn teaches that said messager being usable to exchange control messages with said remote party to ensure that a same bitstream part is used for resynchronization at both said parties (Message structure 20 provides for system security by preventing the deception of receiver 18 by interception, col. 3, lines 50-51).

With respect to claim 14, Khamharn teaches that said messager being usable to vary a control message in accordance with a sub-cycle current at a synchronization loss event, thereby

to control said remote party to resynchroni-ze using a same bitstream part (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 3, lines 13-16).

With respect to claim 15, Khamharn teaches that operable to respond to messages sent by a remote party following said synchronization loss event, to revert to same said bitstream part as said message indicates that said remote party intends to use (In this case, receiver 18 will execute a resynchronization process dependent upon receiving and verifying a second and a third message 20 reception, col. 4, lines 44-47).

With respect to claim 16, Khamharn teaches that circuitry for determining which of itself and said remote party is a transmitting party and being operable to control said synchronization when it is a transmitting party and to respond to control commands of said remote party when said remote party is said transmitting party (Transmitter 12 emits RF signals 16 in response to use activation of one or more buttons 14 associated with transmitter 12. Receiver 18 periodically checks for the presence of a transmission and performs the requested function only if the fields within message structure 20 (FIG. 2) are intended for that particular receiver and contains valid security information, col. 3, lines 1-7).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the above references with to perform and restore synchronization between the transmitter and the receiver.

With respect to claim 17, Khamharn teaches that said synchronized state determiner comprises: a calculation circuit for carrying out an irreversible calculation on any one of said bitstream, said randomization, said key and derivations thereof, and a comparator for comparing a result of said calculation with a result received from said remote party, thereby to determine whether said parties are in synchronization (an initial first sequence number value (SQN1) 28, a random initial state (not shown), and a cryptographic key (not shown), col. 3, lines 27-30).

With respect to claim 18, Khamharn teaches that said irreversible calculation comprises a one-way function (a calculation using an algorithm to combine a cryptographic key with function code 24 and CRC 32, col. 3, lines 46-48).

With respect to claim 24, Khamharn teaches that each selector comprises an address generator and each address generator is identically set (function code 24 which identifies the fuction being requested, col. 3, lines 40-41)

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the above references with to perform and restore synchronization between the transmitter and the receiver.

With respect to claim 25, Khamharn teaches that a controller for exchanging control data between said parties to enable each party to determine that each selector is operating synchronously at each party (transmitting at least a first message from the transmitter to the

receiver; and, in response to the receiver receiving the first message, the receiver detecting the absence of synchronization between the transmitter and the receiver and performing a resynchronization procedure to restore synchronization between the transmitter and the receiver, see abstract)

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the above references with to perform and restore synchronization between the transmitter and the receiver.

With respect to claim 26, Khamharn teaches that redundancy check data, and a hash encoding result, of at least some of the bits from said derived bit source (a cryptographic key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 27, Khamharn teaches that redundancy check data, and a hash encoding result, of at least some of the bits of said randomization (a cryptographic key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 28, Kahmharn teaches that redundancy check data, and a hash encoding result, of at least some of the bits from said key (a cryptographic key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 29, Khamharn teaches that redundancy check data of at least some of said addresses, and a hash encoding result of at least some of said addresses (a cryptographic

key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 30, Khamharn teaches that at each party a resynchronizer operable to determine from said control data that synchronization has been lost between the parties and to regain synchronization based on a predetermined earlier part of said derived bit source (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 4, lines 13-16).

With respect to claim 34, Khamharn teaches that said controller being usable to include in said control messages, data to ensure that a predetermined earlier part of said derived bit source of a same cycle is used for resynchronization at both said parties (In this case, receiver 18 will execute a resynchronization process dependent upon receiving and verifying a second message 20 reception, Co. 4, lines 36-40)

With respect to claim 42, Khamharn teaches that exchanging control data between said parties to enable each party to determine whether they are operating synchronously with said other party (transmitting at least a first message from the transmitter to the receiver; and, in response to the receiver receiving the first message, the receiver detecting the absence of synchronization between the transmitter and the receiver and performing a resynchronization procedure to restore synchronization between the transmitter and the receiver, see abstract).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the above references with to perform and restore synchronization between the transmitter and the receiver.

With respect to claim 43, Khamharn teaches that redundancy check data of at least some of said derived data source, and a hash encoding result of at least some of said derived data source (a cryptographic key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 44, Khamharn teaches that determining from said control data that synchronization has been lost between the parties and regaining synchronization based on a predetermined earlier part of said derived data source (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 3, lines 13-16).

With respect to claim 45, Khamharn teaches that further comprising a step of exchanging said predetermined earlier part of said derived data source at predetermined intervals (sequence of operations for restoring synchronization, such as depressing lock and unlock buttons for a predetermined period of time and waiting for a lock cycle feedback, col. 1, lines 24-27).

With respect to claim 46, Khamharn teaches that determining a possibility of each party being at a different cycle at synchronization loss, and controlling said resynchronization to use a

same predetermined earlier part of said derived data source at both parties (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 3, lines 13-16).

With respect to claim 47, Khamharn teaches that further comprising creating in advance a future cycle's predetermined earlier part of said derived data source for resynchronizing with a party that has already moved to such a cycle (resynchronization process occurs in resynchronization area 52 whereby, subsequent to a first message 20 reception, SQN1 28 received is grater than auto-resync window 48 yet less than SQN2 42, col. 4, lines 41-44).

7. Claims 31-33 and 35-36, are rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla in view of Seheidt and further in view of. Khamharn

With respect to claim 31, Atalla in view of Seheidt teaches the system according to claim 22 but does not teach that at each party a resynchronizer operable to determine from control data exchanged between said parties that synchronization has been lost between said parties and to regain synchronization based on a predetermined earlier part of said derived bit source synchronization

However, Khamharn teaches that at each party a resynchronizer operable to determine from control data exchanged between said parties that synchronization has been lost between said parties and to regain synchronization based on a predetermined earlier part of said derived

bit source synchronization (A first resynchronization process occurs within synchronization window 44, a resynchronization area whereby, subsequent to a first message 20 reception, SQN1 28 received is greater than SQN2 42 by not more than K increments, col. 4, lines 17-21).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the above references with to perform and restore synchronization between the transmitter and the receiver.

With respect to claim 32, Khamharn teaches that said data communication process being arranged in cycles, said predetermined earlier part being exchangeable in each cycle (Current systems require a manual sequence of operations for restoring synchronization, such as depressing lock and unlock buttons for a predetermined period of time and waiting for a lock cycle feedback, col. 1, lines 22-26).

With respect to claim 33, Khamharn et al. teaches that said cycles being arranged into sub-units, each said cycle having an exchange point at its beginning for carrying out said exchange of said predetermined earlier part of said derived bit source (CRC 32 which is a cyclic redundancy check code to permit receiver 18 t validate the integrity of message transmission, col. 3, lines 48-49).

With respect to claim 35, Khamharn teaches that said controller being usable to vary a control message in accordance with a sub-cycle current at a synchronization loss event, thereby to control said remote party to resynchronize using same said predetermined earlier part of said

derived bit source (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 3, lines 13-16).

With respect to claim 36, Khamharn teaches that operable to respond to messages sent by a remote party following said synchronization loss event, to revert to same said predetermined earlier part of said derived bit source as said message indicates that said remote party intends to use (In this case, receiver 18 will execute a resynchronization process dependent upon receiving and verifying a second and a third message 20 reception, col. 4, lines 44-47).

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SIMON KANAAN whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 5712723799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/SIMON KANAAN/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432